REMARKS

Claims 1-8 are currently pending in the application. Claims 1,2, 4, and 7 have been amended to make the claims clearer to the Examiner. However, the instant changes are not being made for reasons related to patentability and they do not narrow the scope of the claims. Additionally, the specification has been amended to correct some minor informalities identified by the Applicants.

Applicants would also like to advise the Examiner that an Information Disclosure Statement was filed on February 14, 2002. It is respectfully requested that in the next communication from the Examiner an initialed copy of the PTO-1449 be returned.

Claims 1-8 stand rejected under 35 U.S.C. 112, second paragraph, for the reasons set forth on page two of the office action. Applicants have amended claims 1 and 2 to help clarify the claims for the Examiner but submit that the original claims as well as the amended claims each particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. Regarding claim 1, there is only a single computer referred to because the issue of who owns the computer is not a part of the claim and the Applicants are not required to specify whether the computer is a buyer's computer or a merchant's computer. In the preferred embodiment, by way of example, the buyer's computer performs all of the recited method steps. As for the remaining claims, when another computer is set forth in the claims, it is identified as either "a broker computer" (claim 2) or "first and second computers" (claim 7).

Claims 1, 4-6 and 8 stand rejected under 35 U.S.C. 102(e) as being anticipated by Downs (6,226,618). This rejection is respectfully traversed.

The Applicants note that Downs is a very long and detailed patent that is directed to an electronic content delivery system (hereinafter "ECDS") that permits digital content to be provided electronically in a secure manner. The ECDS includes a content provider 101, an electronic digital store 103, a clearinghouse 105 and an end user device 109. The content provider hosts (or allows a third party to host) the digital content. The electronic digital store markets the digital content on behalf of the content provider. The clearinghouse is a trusted third party that performs license control functions to ensure that only properly licensed end users can obtain the specified digital

content. Downs discloses that the digital content is ultimately sent from the content provider to the end user via a content secured container 630 while metadata secured containers 620 are made accessible to the end user via the electronic digital store. The metadata secured containers include promotional information about the digital content and perhaps a small portion of the digital content to be accessed by the end user. However, only the content secured containers include an encrypted version of the entire digital content. The containers 620 and 630 are separate data packets.

Claim 1 describes a computer that has downloaded to it a digital content file that includes a digital content product in encoded form and a header that has purchasing information about the digital content product. In Downs, the purchasing information is contained in the metadata container 620 while the encoded digital content product is contained in the contents container 630. These containers are separately downloaded to the end user. Thus, the downloading of the claimed single file is neither taught nor suggested by Downs.

Additionally, claim 1 recites that as the digital content file is downloaded, the header information is read and displayed while the encoded digital content product is concurrently downloaded into the computer. As discussed above, the content secure container 630 and the metadata secure container 620 are downloaded to an end user at different times in the process and therefore the concurrent activities recited in claim 1 are neither taught nor suggested by Downs.

The Examiner refers to Figure 16 for allegedly teaching the reading of the header information with a concurrent downloading of the encoded digital content product. However, such is not the case. Figure 14 and its associated description in the specification do not explicitly discuss whether header information is being read and displayed concurrently with the download of the encrypted product. For example, the header information may have been previously read and displayed and only upon product purchase is the encoded digital content downloaded. In the instant invention, a file with the header and digital content is downloaded to the computer.

Claim 4 is directed to a method that would allow, for example, a third party to access a web site of a merchant to encrypt digital content files at the merchant web site. Thus, the computer is provided with the identification of the merchant's files that require

encryption together with the web site location of the files and information as to how to access those files. The computer connects to the web site, such as through the Internet, and accesses, and encrypts the designated files and stores the encrypted files at the web site. This claim permits remote encrypting of files at a merchant web site.

The Examiner refers to column 26, lines 34-68 for teaching using URL's to point to files at a host site. However, Downs does not teach or suggest the remote computer actuated encryption of designated files as claimed.

Claim 7 is directed to a method whereby encrypted and unencrypted digital content product files are stored at a first computer, such as a merchant computer. Upon request for the encrypted files they are sent to a second computer. However, in the case of the unencrypted digital content product files they are dynamically encrypted prior to being sent to the second computer. This method of distributing digital content using static encrypting and dynamic encrypting is discussed in detail on page 16 of the specification. The specification describes the benefits of this hybrid encrypting of files. That is, static encoding is efficient for content that is not subject to change (such as a particular piece of music) because time is saved if real time encryption is not required. However, constantly changing information, such as stock data, would require a large amount of continuous maintenance to store in encrypted form. Thus, for the constantly changing data, dynamic encryption is best suited since the product is encrypted for each download. The Examiner's reference to the storing of encrypted and unencrypted materials does not address the dynamic encrypting of unencrypted materials together with statically encrypted materials.

In view of the above, it is submitted that independent claims 1, 4, and 7 are neither anticipated by nor rendered obvious in view of Downs. Further, claims 5 and 6 are considered patentable based on their dependency from claim 4 as well as for the specific elements recited which Downs does not teach or suggest. Further, independent claim 8 is considered patentable for the reasons discussed above regarding claim 1 since it is directed to a computer-readable medium incorporating the method steps of claim 1.

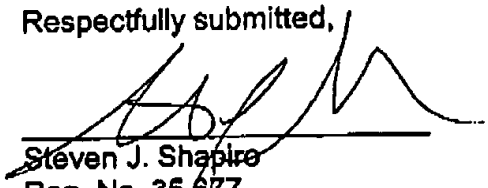
Claims 2 and 3 stand rejected over Downs in view of Blatter (6,016,348). This rejection is respectfully traversed.

It is submitted that Blatter does not correct the deficiencies discussed above with respect to the downloading of the claimed digital content file as discussed above. Thus, claims 2 and 3 are considered patentable based on their dependency from claim 1. Moreover, Blatter does not read and display header information including purchasing information about the product. Rather, Blatter is simply decoding and displaying the video data in real time. Since Blatter is not directed to selling a product, the claimed file structure is not needed.

In summary, it is the Applicants' position that the arguments above overcome the rejections. However, if the Examiner disagrees, the Applicants respectfully request that the Examiner specifically identify those portions of the large Downs reference where specific claim limitations are taught or suggested. Since it is incumbent on the PTO to establish a prima facie case of obviousness, general references to Downs are not considered appropriate.

In view of the above, it is submitted that the application stands in consideration for allowance. Reconsideration of the rejections is respectfully requested and an early notice of allowance earnestly solicited. If however, the Examiner has any additional questions, please contact the undersigned at the number below.

Respectfully submitted,



Steven J. Shapiro
Reg. No. 35,677
Attorney of Record
Telephone (203) 924-3880

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

Version with Markings to Show Changes Made

In the specification:

Last paragraph on page 8, bridging onto page 9:

A description of the operation of the online payment system 100 will now be described with reference to Figures 1-2 and 5-6. At step 500 a registered merchant 106 decides to place an item of digital content (article, music, picture, movie, other data) for sale utilizing the online payment system 100. The merchant 106 uses the encoder utility software 150 provided by the payment broker 118 to encrypt the digital content of the item for sale by first calculating a unique product key "K_{prod}" for the item (step 502). K_{prod} is derived by using the encoder utility software 150 to create a secure one way hash of data known to the merchant such as a product ID, the merchant secret key "K_m", and a randomly generated number. K_{prod} is then used by the encoder utility software 150 to encrypt the digital content of the item using a known encryption algorithm (step 504). Once the item has been encoded, the encoder utility software 150 creates the file 180 to include a length identifier 200, a signed header 202, a product preview 204, and the digitally encoded content 206 (step 506). The length 200 is used to identify the length of the header 202 portion of the file 180. The significance of this field is that it allows the plug-in 178 to know how much information needs to be read in ~~eder~~order to display the header 202 while concurrently downloading the data for the product preview 204 and the encrypted digital content 206. Alternatively, the file length 200 can be used by the plug-in 178 to only download the header 202 and present that information (required to complete the sale) on display 123. The remainder of file 180 (product preview 204 and encrypted digital content 206) are respectively downloaded only if the buyer chooses to view the product preview 206 or buy the digital content item. Accordingly, second and third file lengths can be included as part of the digital file 180 to respectively identify to the plug-in 178 the respective lengths of the product preview 204 and the digital encrypted file 206. These file lengths allow the product preview data 204 to be downloaded and displayed upon request by the buyer without

requiring the encrypted digital content file 206 to be downloaded until a buy decision is made by the buyer. Thus, using the file lengths to delay the downloading of various portions of file 180 greatly improves network performance since selective portions of the file 180 are only downloaded upon command.

Last paragraph on page 11, bridging onto page 12:

Once the buyer decides to purchase the digital content 206 of the downloaded file 180, the plug-in 178 generates a purchase request that is sent to the broker server 132. The purchase request is created by the plug-in 178 by digitally signing information contained in the header 202 such as the product ID and the price together with the buyer ID and signing this information with the private key K_{BV} of the buyer 102 (step 616). In addition to the purchase request, the header 202 information of file 180 is also sent to the broker server 132. The purchase request and header 202 are sent to the broker computer 132 via a SSL (step 618). The broker computer 132 obtains the public key K_{BU} of the buyer from the buyer vault 170 and uses it to verify the signed header information in the purchase request using the same algorithm stored in the decryption unit 164 that the plug-in 178 used to sign the information (step 630). A comparison of the decrypted information is made with the header 202 information included in the purchase request (step 622). If the decrypted header information matches the corresponding header 202 information sent as part of the purchase request, verification of the buyer's purchase request has successfully occurred (step 624). If there is not a match, the transaction is terminated (step ~~624~~625). Assuming verification is successful, the broker computer 132 then calculates a MAC in the same manner that the merchant 106 calculated the MAC contained in the header 202 using the merchant specific data residing in the merchant data base 160 (merchant key Km obtained by correlation to merchant ID in purchase request) together with the other information needed to calculate the MAC and contained in the header 202 (step 626). If the broker calculated MAC matches the MAC in the header (step 628), verification that the header 202 information is actually that of the merchant 106 occurs (step 630). Thus, if an unscrupulous buyer attempted to change, for example, the price in the header 202, a MAC match would not occur and the

transaction would be terminated (step 632). Therefore, a reliable price check mechanism is incorporated in the online payment system 100.

Last Paragraph on Page 13, bridging onto Pages 14 and 15:

Subsequent to the download of the receipt and the product key by the by the buyer computer 122, the plug-in 178 via the browser 176 displays a post sales dialogue box on display 123 (step 800). The post sales dialogue box queries the user as to whether 1) they wish a refund, 2) they wish to take a survey (with an offer to be reimbursed for their time), and 3) the transaction is complete. If the buyer selects a request for refund, a new dialogue box appears prompting the user to select from among a predetermined number of reasons as to why they desire a refund or to enter their own reason (step 810). This information along with the receipt for the item is signed with the private ~~key~~key of the buyer K_{BV} and sent to the broker computer 132 (step 820). The broker computer 132 utilizes the buyer's public key K_{BU} to obtain the refund information and the receipt (step 822) and checks to ensure that 1) the buyer's account is active, 2) the refund request is for a previously purchased item and 3) a refund has not previously been made for that item (step 824). Additionally, the broker computer 132 ensures that any preset period of time associated with how long after purchase a request for refund can be made has not been exceeded (step 824). If any of the above checks fail the buyer 102 is advised that a refund will not be given (step 826). On the other hand, if the checks are all positive, the broker computer 132 debits the refund amount from a dispute account associated with the buyer 102. That is, for each buyer, in addition to their vault 170 there is a dispute account established at the broker computer 132. The dispute account has a threshold value associated with it that is debited each time a refund is given to a buyer. Thus, for a given refund the dispute account and the merchant's account 162 for the merchant 106 selling the particular item are debited by the refund amount (step 828). The money debited from the merchant's account is transferred to the buyer's vault 170 (step 830) and the buyer receives a message on display 123 that the vault has been credited (step 832). However, if the dispute account is decremented to zero or a negative (step 829), a flag associated with the buyer's vault

170 is set from an active status to an inactive status (step 834). At this point in time it is determined if the credit card accepts refunds (step 835), and if it does, any monies in the buyer's vault 170 are refunded to the buyer's default credit card (step 836). If the default credit card does not accept a refund, a message is sent to a general logging device so that a manual refund can be issued (step 838). The buyer 102 then receives a message indicating that their vault is inactive and their remaining money will be credited to the default credit card or returned manually as the case may be (step 840). It is also possible to establish a time limit associated with the threshold value of the dispute account. That is, if the threshold value is not exceeded over a specified period of time, the dispute account is reset an initial value. Moreover, an additional counter can be added at the broker computer 132 for each buyer 102 that keeps track of the number of times a refund has been requested. If the number of requests exceeds a predetermined number, the buyer's vault is rendered inactive. Additionally, while the above described embodiment described the refund account as a descending register which starts at the threshold value and is debited down to zero, one skilled in the art will recognize that the refund account could be an ascending register which adds the refund amounts and inactivates the buyer's vault 170 when the predetermined threshold value is met.

First full Paragraph on Page 16:

In the above described embodiment, the encoded digital content 206 is placed on the web site 181 in encoded form (static encoding). A benefit of static encoding is that no software is required at the host web site 181. Thus, static encoding is good for items that will have no content change such as previously written articles or musical recordings. However, if the item for sale is constantly changing data, such as stock information, the static encoding method is not efficient. In this situation, the encryption utility software 150 would be placed at the host web site 126 and the digital content to be purchased would be encrypted dynamically prior to each download of a file 180 to a

buyer 102. Thus, for each buyer request for a digital content item a new product key K_{prod} is generated. This provides increased security since if K_{prod} is compromised for a single download of a file 180, only that specifically downloaded file 180 is compromised. In the static situation where there is a single K_{prod} associated with a file 180, if K_{prod} is compromised any download of the file 180 is potentially compromised. The disadvantage of the dynamic encoding model as compared to static encoding is that it creates a greater burden on the host server 126. The instant invention recognizes the advantages of static and dynamic encoding and in one embodiment contemplates a web site host 126 that has statically encoded digital content which is of a low value and a stable nature and also provides dynamic encoding of rapidly changing digital content and/or high value digital content items. Since the ultimate file structure 180 resulting from either the dynamic or static encoding is the same, the plug-in 178 can effectively perform its designed functions in either situation.

Last Paragraph on Page 18, bridging onto Page 19:

An alternative method of providing the multiple copy/distribution corporate rate structure is to designate, in the buyer database 168, a designated rate for multiple copies (i.e. ~ 50) that is automatically invoked any time the particular buyer 102 purchases an item. In this situation the buyer 102 would be charged a cost associated with the initial cost of the item as well as the premium charged for the right to make/distribute the designated multiple copies. This feature also permits the customizing of discounts to individual corporations.

In the claims:

1. A method for using a computer to facilitate a transaction between a merchant and a buyer, the method comprising the steps of:

~~inputting~~downloading into the computer a digital content file of the merchant, the digital content file including a header with information related to purchasing a digital content product and the digital content product in encoded form; and

using the computer for reading the downloaded header and displaying at least some of the information related to purchasing the digital content product while concurrently downloading the encoded digital content product into the computer.

2. A method as recited in claim 1, further comprising inputting a request to purchase the digital content product into the computer, outputting from the computer the request to purchase to a broker computer, receiving at the computer from the broker computer a key for decoding the encoded digital content product in response to the request to purchase, and using the key at the computer to decode the encoded digital content product to create a decoded digital content product while concurrently displaying the decoded digital content product.

4. A method for using a computer by a broker to encrypt digital content product files of a merchant that are hosted at a merchant web site, the method comprising the steps of:

inputting into the computer an identification of the digital content product files designated for encryption together with the web site location of the digital content product files and information required to access the digital content product files;

via the computer, connecting to the web site and accessing and encrypting the digital content product files designated for encryption; and

storing the encrypted digital content product files at the web site.

7. A method for distributing from a first computer digital content products for purchase, the method comprising the steps of:

encrypting a first digital content product file;

statically storing the encrypted first digital content product file at the first computer;

storing a second digital content product file in unencrypted form at the first

computer; and

inputting a request into the first computer for downloading from the first computer to a second computer at least one of the encrypted first digital content product file and the second digital content product file;

wherein at times when the request is for the encrypted first digital content product file downloading the ~~first~~ encrypted first digital content file to athe second computer, and at times when the request is for the second digital content product file dynamically encrypting the second digital content product file and sending the second digital content product file in encrypted form to the second computer while maintaining the storing of the second digital content product file in unencrypted form at the first computer.